Brief
March 2001
Senate Research Center • Sam Houston Bldg. • Suite 575 • 201 E. 14th Street • Austin, TX 78701 • 512.463.0087 • Fax: 512.463.1271 • TDD: 800.735.2989

A Handbook on Privacy

Federal and State Legislation

The right to privacy is not an expressly stated right in the United States Constitution. However, the United States Supreme Court has found and delineated an implied constitutional right of privacy. In the 1977 case *Whalen v. Roe* (See Box on *Whalen*), the U.S. Supreme Court distinguished between two interests within the "zone of privacy" protected by the Constitution. The first zone refers to a person's interest in keeping certain matters confidential, such as those that may be considered sensitive or personal. The second zone involves a person's right to make certain kinds of decisions, such as those related to marriage or procreation.

Although the Texas Constitution lacks explicit privacy guarantees, the Texas Supreme Court has followed the lead of the highest federal court, finding that the Texas Constitution contains several implicit provisions for privacy.

Recent national polls indicate a heightened public concern with personal information and its security. A series of national public opinion polls conducted by Louis Harris and Associates documents a rising level of public concern about privacy, growing from 64 percent in 1978, to 82 percent in 1995. Over 80 percent of persons surveyed in 1999 agreed with the statement that they had "lost all control over their personal information." In March 2000, a *Business Week*/Harris Poll revealed about 90 percent of participants were concerned about the exchange of personal information between commercial websites. Over half of those questioned thought that government should pass laws regulating the way in which personal information is collected and used.[1]

But those who advocate privacy laws have their opponents. The very nature of our political system creates an inherent tension between a private citizen's "right to be left alone" and the public's "right to know." An open and transparent government safeguards against the abuse of political power and misuse of public resources, and holds public officials and servants accountable to the people. In Texas, the open records laws, known as the Texas Public Information Act (Chapter 552, Texas Government Code) presumes that information in the possession of a government entity is public information, unless specifically exempted from disclosure by court order, under common law, constitutional doctrine, or through specific exemptions.

However, an open and transparent government often exposes individuals' personal lives to public scrutiny. In many cases, that exposure is reasonable and legitimate. Government agencies are now able to share information with one another for purposes such as enhancing public safety and detecting fraud. For example, in order to hire safe bus drivers, a school district may compare applications with state driver's license records. However, disclosing personal information can be the subject of dispute. For instance, an Ohio woman sued information database supplier Metromail Corporation in 1996. Metromail used Texas state prison inmates to type warranty cards and consumer surveys into its database. One convicted rapist used details gleaned from the woman's life to send her explicit and threatening letters, containing such intimate details as what kind of bath soap she used.[2] Metromail, in a Travis County court settlement, agreed to disclose in clear language how it would use personal information.[3]

This *Issue Brief* discusses federal and state legislation and includes:

- **Privacy Legislation Overview**
- **Landmark Federal Legislation on Personal Information**
- **Recent Federal Privacy Legislation**
- **Recent Legislation in Other States**
- **Glossary of Privacy Terms and Websites on Privacy**

Brief Privacy

Privacy Legislation Overview

Recent technological advances in data collection and exchange have created a heightened concern over the erosion of individual privacy. Information and services that once required a trip to a business, public archives, or state agency, can now be accessed instantly through the Internet. In many ways, this advance provides citizens an opportunity to access government services and purchase consumer goods in a more convenient fashion. However, the downside of technology is a loss of control over personal information. To address the issue of privacy concerns, several countries developed certain fundamental principles regarding the collection, use, and dissemination of personal information, and included the following:

- ***Notice/Awareness*** - Individuals should be given notice of an entity's information practices before they divulge any personal information.
- ***Choice/Consent*** - Individuals should be given options as to the uses of any personal information collected from them.
- ***Access/Participation*** - Individuals should be able both to access data about themselves and to contest the accuracy and completeness of the data.
- ***Enforcement/Redress*** - Privacy protections can be effective only if an enforcement mechanism is in place.

Some aspects of these principles are codified in federal law as the Privacy Act of 1974. The federal agency that monitors privacy is the Federal Trade Commission (FTC). Last year, the FTC released its third report on privacy, *Privacy Online: Fair Information Practices in the Electronic Marketplace*, and recommended several changes in the proposed federal law regarding the collection and dissemination of personal information. The proposed legislative changes are included in H.R. 89, recently introduced in the 107th Congress. The Act includes the following:

- Makes it unlawful for an operator of a website or online service to collect, use, or disclose personal information concerning an individual, ages 13 years, and above.
- Provides incentives for self-regulation by operators to implement information protection.
- Authorizes states to enforce regulations by bringing actions on behalf of residents.

Technology has made information gathering easier and less cumbersome. Today, separate and unrelated bits of information are now capable of being linked by data mining and data merging. Electronic connections of county courthouse records, with state and federal databases combined with corporate surveys and records, provide substantial details on individuals and organizations. Federal and state legislation continues to address the rapid changes in computer technology and other information gathering systems.

For example, the FTC concluded in its latest report to the United States Congress that self-regulatory measures had fallen short and legislative actions were required to ensure adequate protection of consumer privacy. However, Commissioner Swindle dissented from the FTC recommendations. In his dissent, Commissioner Swindle stated that the report fails to consider the cost of legislation in comparison to the asserted benefits of enhancing electronic commerce. Swindle stated that the report relies on skewed descriptions of an FTC 2000 survey on privacy by misrepresenting consumer concerns about privacy as the basis of a remarkably broad legislative recommendation.

In addition, the United States Department of Justice's Bureau of Justice Statistics recently launched a two-year study by the National Task Force on Privacy, Technology and Criminal Justice Information, to address the growth of Internet access and issues related to privacy protections. The Task Force's initial proposal included the recommendation to seal or purge criminal histories when they no longer serve an important public safety issue or other public policy interest.

Whalen v. Roe

The right of informational privacy was first addressed by the United States Supreme Court in *Whalen v. Roe*. This case involved a New York statute requiring physicians to submit copies of prescriptions for abused drugs to the state for inclusion in a centralized computer file. Although the court upheld the statute, finding that New York's interest in experimenting with solutions to control the distribution of dangerous drugs was a legitimate exercise of the state's police power; the court affirmed the right of an individual to have his personal information kept private. The court stated:

> *"We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files. The collection of taxes, the distribution of welfare and social security benefits, the supervision of public health, the direction of our Armed Forces, and the enforcement of the criminal laws all require the orderly preservation of great quantities of information, much of which is personal in character and potentially embarrassing or harmful if disclosed. The right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures."*
>
> —*Whalen v. Roe*, 429 U.S. 589 (1977)

Landmark Federal Privacy Legislation

Gramm-Leach-Bliley/Financial Modernization Act, 1999 (GLBA)

GLBA regulates the dissemination of certain nonpublic personal information by financial institutions, such as banks, savings associations, credit unions, investment companies, and insurance companies, to unaffiliated third parties. Generally, disclosures to such third parties are permitted only if the financial institutions give notice to the consumer and provide consumers with the opportunity to "opt out" (the information is public unless consumer says otherwise) of such disclosures. The law is controversial, with critics asserting that the privacy protections are too lax by pointing out that financial institutions are free to share such information with affiliated companies.

Privacy

The statute and subsequent regulations being formulated by the National Association of Insurance Commissioners (NAIC) present the most immediate compliance requirement for the insurance industry, with a July 2001 deadline imposed on the states. With GLBA, the financial services sector became the first national industry group to face formal statutory requirements concerning privacy.[4] In order to comply with new GLBA rules, NAIC's model distinguishes "financial" information from "health" information. Federal GLBA regulations include health information within their scope of protection.

The NAIC model, while generally tracing federal rules for financial information, creates "opt-in" (the information is private unless consumer says otherwise) requirements for the disclosure of health information, with certain exceptions (e.g. claims administration, disease management, policyholder service functions, and auditing and fraud investigations).

Children's Online Privacy Protection Act (COPPA), 1998

The COPPA makes it unlawful for an operator of a web site to collect personal information from a child under 13 years of age. In general, a web site that is directed at children or knowingly collects this information from children must obtain verifiable parental consent for the collection, use, or disclosure of personal information. The law's requirements are triggered at the time the data is collected.

Identity Theft and Assumption Deterrence Act (ITADA), 1998

ITADA makes identity theft a federal crime with penalties up to 15 years imprisonment and a maximum fine of $250,000. It establishes that the person whose identity was stolen is a true victim. Previously, only the credit grantors who suffered monetary losses were considered victims.

Health Insurance Portability and Accountability Act (HIPAA), 1996

Congress addressed the issue of rapidly changing health information systems in the HIPAA. The Act directs the United States Department of Health and Human Services (HHS) to issue standards that facilitate the electronic exchange of information and transactions carried out by health plans, health care clearinghouses, and health care providers.

HHS set forth privacy standards under the Act in December 2000 and the rules are scheduled to take effect in April 2001. President Bush reopened public comments on the rules amid a number of arguments concerning implementation of the rules. The federal rules do not preempt more stringent state laws relating to the privacy of individually identifiable health information.

Driver's Privacy Protection Act, 1994

The federal Driver's Privacy Protection Act of 1994 restricts the state's ability to disclose a driver's personal information without the driver's consent, generally prohibiting the knowing disclosure of personal information about any individual obtained in connection with a motor vehicle record (MVR).

The Act defines a "motor vehicle record" as any record that pertains to a motor vehicle operator's permit, motor vehicle title, motor vehicle registration, or identification care issued by a department of motor vehicles. "Personal information" is defined under the Act as any information that identifies an individual's photograph, social security number, driver identification number, name, address (except for the five-digit zip code), telephone number, and medical or disability information, but not including information on vehicular accidents, driving violations, and driver's status.

Fair Credit Reporting Act (FCRA), 1992

The FCRA was enacted to protect the privacy of consumers' credit information, and generally applies only to individuals, not corporations and partnerships.

Telephone Consumer Protection Act (TCPA), 1991

TCPA addresses consumer concerns about unsolicited telephone marketing by imposing restrictions on the use of automatic telephone dialing systems (also called autodialers), artificial or prerecorded voice messages, and telephone facsimile (fax) machines to send unsolicited advertisements.

Video Privacy Protection Act, 1988

Title 18, Section 2710, of the United States Code, generally bars businesses which rent or sell videotapes from knowingly disclosing "personally identifiable information" about their customers, which includes information about the specific video materials a customer bought or rented. Exceptions include a response to a court order.

Electronic Communications Privacy Act (ECPA), 1986

ECPA extended protections to e-mail and other new technology, but continued to allow companies to monitor their employees' electronic communications, including e-mails. ECPA applies only to actions by the government, and does not apply to private employers.

Right to Financial Privacy Act, 1978

The act, largely procedural, was Congress' response to a United State Supreme Court decision that found bank customers had no legal right of privacy for their financial information when law enforcement purposes deemed the release necessary. The law requires government agencies to provide notice and an opportunity to object before these types of personal financial information may be disclosed, under certain conditions.

Family Educational Rights and Privacy Act (FERPA), 1974

FERPA protects both parents' access to and confidentiality of educational records. Schools may not release grades, directory information such as names, addresses, telephone listings, dates and places of birth, or major field of study, among others.

Privacy Act, 1974

This act governs the collection and dissemination of personal information by federal agencies and also provides civil and criminal penalties and remedies. Under the Act, citizens are expressly given

Privacy

the right to know what information the government has collected about them, how it is used, and examine and correct such data. However, the Act covers only the federal government, and not the private sector, and thus, by many is "considered weak and full of loopholes." [5]

National Crime Prevention and Privacy Compact, 2000-2001

The National Crime Prevention and Privacy Compact is a proposed legislative model for creating a cooperative exchange system of criminal data between the states and the federal government. For example, if a Texas school district made inquiries about a potential employee's criminal record in Michigan, then that data would be subject to Texas's privacy laws. However, if a Michigan school district made inquiries about a potential employee's criminal record in Texas, then Michigan's privacy laws would prevail. Availability of certain information would depend entirely on individual state privacy laws. As of January 2001, nine states (Colorado, Connecticut, Florida, Georgia, Iowa, Missouri, Montana, Nevada, and South Carolina) have ratified the compact. Six states, including Texas, are presently considering legislation.

Recent Federal Privacy Legislation: 105th and 106th Congress

Congress, over the past two sessions, has enacted a number of federal laws that address personal privacy protections. This section briefly discusses some of the major privacy enactments.

The 105th Congress enacted the Taxpayer Browsing Protection Act (H.R. 1226), which bars federal officers and employees from unauthorized inspections of tax returns or tax return information.

The 106th Congress passed the following bills impacting personal privacy:

- **The Department of Transportation and Related Agencies Appropriation Act, 2000 (H.R. 2084)** provides that no recipient of funds under this act may disseminate driver's license personal information for any use not permitted under federal law without the express consent of that person (except regarding the use of organ donation information).
- **H.R. 3194** amended the Communications Act of 1934 by barring the distribution of funds to any public broadcasting entity that shares contributor names or other personal information with any political candidate, party, committee, or any nonaffiliated third party unless the donor is given the opportunity to direct that such information not be disclosed.
- **H.R. 4576** bars the use of the funds provided under this act for the transfer, release, or disclosure of an individual's medical records without the individual's consent to any individual or entity outside the Department of Defense for any non-national security or non-law enforcement purpose.
- **H.R. 4640** concerns the collection and analysis of DNA samples from certain violent and sexual offenders for use in the DNA Index System of the Federal Bureau of Investigation (FBI) and contains certain privacy protections.

DNA

Deoxyribonucleic acid (DNA) is a biological marker being used throughout the criminal justice system to identify and convict criminals and exonerate innocent persons. One issue in the collection and dissemination of DNA evidence is the need to protect individual privacy.

The Violent Crime Control and Law Enforcement Act of 1994 (Act) authorizes the FBI to index DNA identification records of persons convicted of crimes and analyze DNA samples recovered from crime scenes and unidentified human remains. DNA identification records and analyses maintained by federal, state, and local criminal justice agencies may be included only if those agencies implement rules limiting the disclosure of stored DNA samples and DNA analyses only to criminal justice agencies for law enforcement purposes, in judicial proceedings, and for criminal defense purposes; the rules may also allow disclosure for a population statistics database and for certain other purposes if personally identifiable information is removed. If these privacy requirements are not met, access to the index can be denied. According to the FBI, all 50 states have enacted DNA database laws requiring the collection of a DNA sample from specified categories of convicted offenders; 46 of these states limit access to these DNA records, either by designating them as confidential or permitting access only for certain authorized purposes. At least half of these state laws contain provisions that are more restrictive than those in the Act. In 32 states, there are penalties for the unauthorized disclosure of DNA information.

Texas currently operates a central database for state DNA records. The main purpose of this database is to assist federal, state and local law enforcement agencies in the investigation or prosecution of sex-related offenses or other offenses in which biological evidence is recovered. The state database must be compatible with the FBI database to allow the exchange and storage of DNA information. DNA records stored in the database are confidential and not subject to disclosure under the state's open records law.

States with Constitutional Provisions Granting a General Right of Privacy

Some states have done more than simply recognize an implied constitutional right of privacy. Eight states—Alaska, Arizona, California, Hawaii, Illinois, Louisiana, Montana, and South Carolina—have state constitutional provisions that expressly recognize a general right of privacy. H.J.R. 15, submitted this session by Representative Hupp, would amend the Texas Constitution to recognize an individual's right of privacy. The proposed amendment provides that this right cannot be infringed upon without a compelling state interest that may not be achieved in a less intrusive and more reasonable manner.

Privacy

Recent Privacy Legislation In Other States

This section highlights some of the most important pieces of legislation enacted among state legislatures from January 1, 1999 to September 2000. The discussion focuses on privacy legislation and not on agency rules and regulations developed by executive departments, and legal interpretations of privacy laws or rules. StateScape, a legislative tracking service, reported during the summer of 2000 that more than 375 privacy bills were introduced in legislatures, and more are likely to be filed during the 2001 legislative sessions. At least nine states have appointed special task forces to explore the issue and report back to the legislature during the 2001 session.[6] One of the difficulties that StateScape and other legislative tracking services face, however, is identifying what types of bills qualify as privacy bills. Privacy definitions vary widely and differ among analysts.[7] With this *caveat* in mind, the following are significant state statutes affecting personal information. The list below is based on information from legislative tracking services, the National Conference of State Legislatures, and Texas Senate Research Center analysis.

GENERAL PRIVACY

California

AB 724 (10/7/99) Protects personal information gathered by government on the Internet; requires Internet disclosures about licensed professionals.

AB 1862 (9/24/00) [also in Criminal Justice] Provides for an identity theft victim database to be maintained by the Department of Justice.

AB 1897 (9/29/00) [also in Criminal Justice] Establishes procedural remedies to assist victims of identity theft.

AB 2246 (9/30/00) Requires a business to ensure the privacy of a customer's personal information, by restricting access to the record prior to its destruction and shredding, erasing, or otherwise modifying the customer record to make information unreadable or undecipherable through any means.

SB 1724 (9/30/00) Prohibits the unrelated use, as defined, and the disclosure, including internal disclosures and those made to subsidiaries or affiliates, of information obtained from a tax return or submitted by a consumer, including that obtained through an electronic medium, in connection with a financial or other business-related transaction.

Connecticut

HB 5893 (5/8/00) Prohibits state agencies from disclosing an individual's photograph or computerized image in connection with issuance of ID card, or other document by such state agency, unless an individual consents.

Delaware

SB 379 (7/26/00) Strengthens disclosure protection for personal information in driver and vehicle records.

Florida

HB 439 (6/16/00) Provides exemptions from public records requirements for investigations of a certified capital company, including social security numbers.

Maryland

SB 199 (4/25/00) Requires state government units to post privacy policies and specifies certain rules for government personal information collection.

HB 1421 (5/18/00) Protects confidentiality of taxpayer information and certain privacy rights of consumers.

Utah

SB 390 (4/7/00), Provides that electronic toll collection records that identify an individual, vehicle, or travel, are exempt from disclosure under the Freedom of Information Act.

Virginia

HB 513 (4/4/00) Directs every public body that has an Internet website to develop an Internet privacy policy (Policy) and an Internet privacy policy statement. The statement, which explains the Policy, shall be posted on the public body's website in a conspicuous manner.

Washington

EO5 (4/25/00) Requires state agencies to eliminate use of social security numbers from public documents; prohibits sales and limits collection and retention of personal information.

HB 2792 (3/22/00) Provides that the following are exempt from public disclosure: credit card numbers, debit card numbers, electronic check numbers, card expiration dates, or bank or other financial account numbers supplied to an agency for the purpose of electronic transfer of funds, except when disclosure is expressly required by law.

West Virginia

SB 577 (4/4/00) Provides confidentiality protection for records such as food stamps, child support or Medicaid.

Wisconsin

AB 315 (4/24/00) Prohibits the Department of Transportation from providing any person with written or electronic information compiled or maintained by the department that contains specified personal identifiers.

CRIMINAL JUSTICE

California

AB 1862 (see above)
AB 1897 (see above)

South Carolina

SB 403 (7/22/99) Limits access to abuse and neglect reports on foster children.

BANKING

California

AB 2869 (9/29/00) Changes notice procedures under the Credit Card Full Disclosure Act.

Connecticut

HB 5586 (5/26/00) Protects consumers from nonconsensual disclosure of personal financial information.

Washington

HB 1250 (5/17/99) Imposes duties on holders of financial information to protect it from improper use or release.

HB 2792 (3/22/00) Exempts the inspection of credit card or financial account information copied and provided to an agency for electronic transfer of funds.

Brief Privacy

IDENTIFY THEFT

Delaware

HB 437 (5/19/00) Creates a crime of identity theft to include theft of electronic identification information, e-mail address, and computer password.

Pennsylvania

HB 945 (5/22/00) Defines the crime of identity theft to include information stored on a computer disk, computer system, computer printout, or any other electronic means.

Rhode Island

HB 7535 (7/6/00) Enacts the Impersonation and Identity Fraud Act, which includes electronic identification numbers and telecommunication identifying information.

South Carolina

HB 3509 (5/30/00) Creates the Personal Financial Security Act, which prohibits theft of identifying information including digital signatures and electronic identifying information.

South Dakota

SB 20 (2/28/00) Creates a crime of identity theft including the theft of user names and identifications.

INSURANCE

California

SB 2166 (9/29/99) Amends Consumer Credit Reporting Agencies Act to prohibit reporting medical information for insurance purposes without individual consent.

Hawaii

HB 351 (6/24/99) Protects the privacy of health care information.

South Carolina

HB 3498 (7/7/99) Prevents transfer of prescription drug information without consent.

South Dakota

HB 1175 (3/11/00) Authorizes Division of Insurance to promulgate rules on privacy of medical records.

MEDICAL

California

AB 1836 (9/30/00) Amends Confidentiality of Medical Information Act to permit transfers without authorization to contractors and others.

SB 1903 (9/30/00) Amends Confidentiality of Medical Information Act to require corporations to provide copies of medical profiles to patients.

Florida

SB 1956 (6/20/00) Provides for the constitutional right of privacy to medical records.

SB 2034 (6/27/00) Specifies circumstances in which the confidentiality of medical records may be compromised to establish an immunization registry or a brain and spinal cord injury program.

Georgia

HB 1300 (5/1/00) Protects personal and research information of persons involved in medical research projects.

Hawaii

HB 351 (6/24/99) Protects privacy of health care information.

Maryland

SB 371 (5/11/00) Prohibits disclosure by sale, rental, or barter of certain medical records and otherwise regulates privacy of medical records.

Massachusetts

HB 5416 (8/22/00) Restricts disclosure and use of genetic test results.

MISCELLANEOUS

Washington

SB 6459 (3/22/00) Prohibits any person to knowingly use a means of identification of another person to solicit unauthorized mail with the intent to annoy, harass, intimidate, torment, or embarrass that person, and civil damages for violations.

Genetic Testing

On Friday, February 9, 2001, the United States Equal Employment Opportunity Commission (EEOC) filed its first court challenge to genetic testing, seeking a preliminary injunction against Burlington Northern/Santa Fe Railroad's genetic testing of employees who filed claims for certain work-related injuries. According to the petition, the railroad has a nationwide policy of requiring employees who have submitted work-related claims for carpal tunnel syndrome to provide blood samples. The samples undergo a genetic test for Chromosome 17 deletion, which is claimed to predict some forms of carpal tunnel syndrome. The action alleges that the employees were not told of the genetic testing or asked for their consent, and at least one individual who refused to provide a blood sample because he suspected it would be used for genetic testing has been threatened with discharge if he fails to submit a sample. The EEOC asserts that basing employment decisions on genetic testing violates the American with Disabilities Act, which prohibits discrimination in employment against qualified individuals with disabilities. Further information is available on EEOC's website at **http://www.eeoc.gov**.

Privacy

Striking a Balance between Public and Private Information

Balancing the public's access to information and the rights of individuals to protect their own information may be finding a solution in the market. Toby Lester, in a March, 2001 article, observes that "the market for goods and services that protect privacy is surging; entrepreneurs are realizing that privacy and technology are not fundamentally at odds and that, in fact, expectations of privacy have in large measure always been created or broadened by the arrival of new technologies…. Billions of dollars are at stake. A new sector of the economy seems to be coming into being. Among entrepreneurs and venture capitalists it already has a name. It's known as the privacy space." [9] Business opportunities are expanding into software designed to erase and encrypt confidential information while entire companies are focusing on maintaining confidential records and information.

But lost somewhere in the corporate privacy space is an individual's right of informational privacy. While privacy may indeed become a billion dollar industry, the issue remains the extent an individual's personal records are accessible by corporations and governmental bodies. Not all individuals are capable of purchasing privacy software or hiring a corporation to maintain their confidentiality. If industry and government have access to this technology, it begs the question of who makes the decision as to where the distinction between information that should be disclosed and information that should remain confidential rests.

In many ways, the idea of government and industry delineating between public and private information is an inherent contradiction. For example, it is essential that both government and industry have access to personal information. "This aspect of government [and industry] is a natural one: personal information is as necessary and as valuable to efficient government as to efficient business." [10] In fact, both industry and government could operate more effectively if they were able to completely monitor and track the daily activities of consumers and citizens. Yet government and industry are also the very entities citizens must rely upon to establish limits on the personal information they access. Perhaps this is why "there are plenty of people who take a decidedly dark view of it, and who therefore have very little faith in the ability of the political system to protect privacy." [11]

But all is not doom and gloom for individual privacy. As the United States Supreme Court in *Whalen v. Roe* stated, "the right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures." As lawmakers and corporate leaders face policy and business decisions, they must also face the consequences of those decisions as citizens and consumers. Perhaps this is the reason lawmakers are now passing and considering a variety of privacy laws and why corporations are purchasing privacy software, hiring privacy managers, clarifying their privacy policies, and maintaining more confidential records or employee information. Whether the market's self-regulatory actions to maintain confidentiality or government efforts to protect personal information are successful will remain a recurring issue for policymakers.

What is happening on privacy issues in Texas? A companion brief will discuss the policy debates in Texas on banking, insurance, criminal justice, and health issues.

—by **Senate Research Center**

Banking and Insurance - Dunya McCammon Bean
Criminal Justice - Rita Aguilar
Education - Betsy Heard
General Research - Mahan Farmaian
General Research - Stephen Boske
Health - David Thomason
Open Records - Sharon H. Weintraub
Technology - J. Joseph Stewart

Privacy

End Notes

[1]Department of Health and Human Services, *Federal Register*, 45 CFR Part 160 and 16, "Standards for Privacy of Individually Identifiable Health Information; Final Rule," 82465.

[2]*Los Angeles Times*, June 24, 2000.

[3]*Washington Post*, September 22, 1999.

[4]Nahra, Kirk. "What Every Insurer Needs to know About Privacy," Mealey's *Emerging Insurance Disputes*, 5.

[5]Sykes, Charles. *The End of Privacy*, (St. Martin's Press, 1999), 85.

[6]Conte, Christopher, "The Privacy Panic," *Governing* (December 2000), 24.

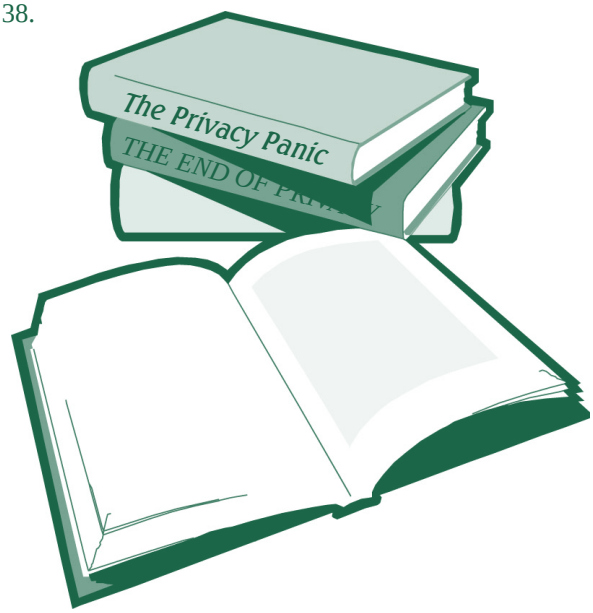
[7]Wiley, Rein and Fielding, "State-Enacted Privacy Statutes," 2.

[8]Definitions drawn from various sources.

[9]Toby Lester, "The Reinvention of Privacy," *Atlantic Monthly* (March, 2001) 28.

[10]Ibid, 38.

[11]Ibid, 38.



Useful Web Sites

www.epic.org Electronic Privacy Information Center

www.healthprivacy.org Georgetown University Health Policy Program

www.computerprivacy.org Americans for Computer Privacy

www.privacy.org Electronic Privacy Information Center

www.privacyheadquarters.com Bankers System, Inc.

www.usdoj.gov/ola/compact United States Department of Justice

aclu.org/issues/privacy/html American Civil Liberties Union

www.aarp.org/bulletin/mar00/privacy.html American Association of Retired Persons

Brief *is a Senate Research Center Publication of the Texas Senate*

Layout and design by Hector R. Meza, Publications Coordinator

Brief

Privacy

Privacy Legislation Introduced in the Current 107th United States Congress

Bill #	Summary	Committee Referred
H.R. 89	**Online Privacy Protection Act of 2001** Requires the FTC protect the privacy of personal information collected from and about individuals who are not covered by the Children's Online Privacy Protection Act.	Energy and Commerce (1/3/2001)
H.R. 91	**Social Security On-Line Privacy Protection Act** To regulate the use by interactive computer services of Social Security account numbers and related personally identifiable information.	Energy and Commerce (1/3/2001)
H.R. 112	**Electronic Privacy Protection Act** To prohibit the making, importation, exportation, distribution offer for sale, or installation, use of an information collection device without proper labeling or notice and consent.	Energy and Commerce (1/3/2001)
H.R. 199	**Law Enforcement Officers Privacy Protection Act** Amends rule 26 of the Federal Rules of Civil Procedure to provide for the confidentiality of a personnel record or personal information of a law enforcement officer.	Judiciary (1/3/2001)
H.R. 220	**Identity Theft Protection Act** Amend Title II of the Social Security Act and Internal Revenue Code of 1986 to protect the integrity and confidentiality of Social Security account numbers issued under such title, to prohibit the establishment in the Federal Government of any uniform national identifying number, and to prohibit Federal agencies from imposing standards for identification of individuals on other agencies or persons.	Ways and Means (1/3/2001)
H.R. 237	**Consumer Internet Privacy Enhancement Act** To protect the privacy of consumers who use the Internet.	Energy and Commerce (1/20/2001)
H.R. 260	**Wireless Privacy Protection Act of 2001** To require customer consent to the provision of wireless call location information.	Energy and Commerce (1/30/2001)
H.R. 347	**Consumer Online Privacy and Disclosure Act** To require the Federal Trade Commission to prescribe regulations to protect the privacy of personal information.	Energy and Commerce (1/3/2001)
H.R. 583	**Privacy Commission Act** To establish the Commission for the Comprehensive Study of Privacy Protection.	Government Reform (2/13/2001)
H.R. 602	**Genetic Nondiscrimination in Health Insurance and Employment Act** To prohibit discrimination on the basis of genetic information with respect to health insurance.	Energy and Commerce Ways and Means Education and Workforce (2/13/2001)
S. 30	**Financial Information Privacy Protection Act of 2001** A bill to strengthen control by consumers over the use and disclosure of their personal financial and health information by financial institutions, and for other purposes.	Banking, Housing, and Urban Affairs (1/22/2001)
S. 197	**Spyware Control and Privacy Protection Act of 2001** To provide for the disclosure of the collection of information (1/29/2001) through computer software and other purposes.	Commerce, Science, and Transportation (1/29/2001)
S. 290	**Student Privacy Protection Act** To increase parental involvement and protect student privacy.	Health, Education, Labor, and Pensions (2/8/2001)
S. 318	**Genetic Nondiscrimination in Health Insurance and Employment Act** To prohibit discrimination on the basis of genetic information with respect to health insurance.	Health, Education, Labor and Pensions (2/13/2001)
S. 324	**Social Security Privacy Act** A bill to amend the Gramm Leach Bliley Act, to prohibit the sale and purchase of the social security number of an individual by a financial institution, to include social security numbers in the definition of nonpublic personal information and for other purposes.	Banking, Housing, Urban Affairs (2/14/2001)

Brief

Privacy

Glossary of Terms[8]

Anonymizers - allow Internet users to conceal their Internet Protocol (see below). The service is similar to "call blocking" for telephones by ensuring the privacy of a user's computer name, domain name, and IP address. By concealing the IP address, personal identity is virtually impossible to discover.

Clear GIFs or web bugs - are invisible graphic files embedded in a web site that allows a site other than the one being visited to track activities. These invisible graphics, each just one pixel by one pixel, allow the potential that a cookie from a site could be placed on a user's hard drive without the user's knowledge.

Consent - concerns the extent to which individuals willingly and knowingly agree to the disclosure of their personal information. Consent can be written, or express. But consent can also be implied and tacit as a person may infer from someone's actions that they have granted consent. Consent is an area of considerable legal debate and an equally contentious issue in the area of releasing personal information. For example, if someone allows her physician to test for a particular disease, is that individual consenting to allow all interested parties (e.g. pharmaceutical companies, insurance companies, places of employment) access to that information?

Cookies - tiny data files that are created on a user's hard drive by a web site, usually the first time the site is visited. It typically contains a unique tracking number that allows the site to identify the user, though not by real name unless the user provides that information to the web site specifically. Cookies allow web sites to tailor information specifically to the user, such as stock quotes, sports scores for favorite teams, or pages that have been updated since the user's last visit. They can also be used to create a dossier of pages viewed, links clicked, and items purchased.

Cookie Crumblers - software designed to seek out and eliminate embedded cookies on a computer hard drive.

Data Matching - (or data merging) cross-checking one set of data with another set of data for potential overlaps. For instance, Wisconsin uses data matching to check driver's license information against driving records and crime data. To capture lost revenue, Wisconsin matches the names of lottery winners against the list of delinquent taxpayers.

Data Mining - uses statistical techniques to discover patterns in data drawn from unrelated databases, and makes inferences about details of people's lives that the subjects never agreed to disclose. For example, tax departments could use data mining to find that people who own boats and have vanity license plates are more likely to underreport their income. This information could allow tax departments to target more precisely where their tax audits would be conducted.

Data Security - the level to which personal information is safe from unauthorized use or access. For example, a code may be required to access certain personal information as a security device. Data could be secure, yet not deemed confidential, or vice-versa, data could be confidential data, but not secure.

Deidentified - protected information that a good faith effort has been made to evaluate the risk that an individual's personal information will be linked to that specific individual. For example, a medical study may evaluate the effects of a drug on an experimental group's disease. If that information is deidentified, then the individual's names and personal identifiers will be excluded. Individuals may be given a number or code as part of the study to protect their identity from being released. The term can include aggregate statistics, health information, information for which random or fictitious alternatives have been substituted for personally identifiable information. See reidentification.

Expungement - or expunction, as it is more commonly called, generally refers to the process by which, upon request by the defendant, the court may order the records of a criminal conviction to be physically destroyed or sealed from files, computers, or other depositories. In some states, expungement is also available for arrested persons not ultimately convicted or in the event of an unlawful arrest. By having their criminal records legally deleted, individuals are able to represent in sworn statements that they have never committed the act subject to the expunction.

Internet Protocol (IP) - abbreviation for Internet Protocol, allows an Internet user to address and drop a package in the system, but there is no direct link between the user and the recipient. TCP/IP, on the other hand, establishes a connection between two hosts so that they can send messages back and forth for a period of time.

Opt In - individual personal information is private unless the consumer says otherwise (written or express).

Opt Out - personal information can be disclosed, or made public, unless the consumer states otherwise.

Reidentification - an attempt to ascertain the identity of the individual who is the subject of protected information, or any specific data.

In Oregon's Lane County, data mining is being used to piece together information from 30 different social agencies to create an early-warning system for child abuse. Children and families who are in trouble often have numerous contacts with social agencies; a father visits a drug or alcohol-treatment facility, for instance, or a wife seeks counseling for depressing, or a child misbehaves in school. Seen in isolation from each other, such contacts may not seem problematic. But when separate encounters with service providers are connected to form a larger picture, they may point to a more serious problem. Officials in Lane County believe certain combinations of variables will lead them to children who face the most serious risk of abuse, and service agencies can then intervene before it is too late. Christopher Conte, "The Privacy Panic," *Governing*, (December 2000), 21.